iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XI **Month of publication:** November 2017

DOI: http://doi.org/10.22214/ijraset.2017.11054

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

Attribute Based Access to Scalable Media

Mr. Lokesh khubalkar[1], Mr. Mrutyunjay Meshram[2], Mr. Narendra Rewatkar[3], Mr. Swapnil Mahant4, Prof. Ankita Kotalwar[5]

[1,2,3,4] *Final Years BE Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur, India.*

[5] *Assistant professor, Department of Computer Science and Engineering, Nagpur Institute of Technology, Nagpur, India.*

Abstract: Cloud computing is concept that treats the resources on the Internet. In this paper Attribute-Based access to the media in the cloud where it uses cipher-text policy Attribute-Based Encryption (CP-ABE) technique to create an access control structure by using the algorithms in the access policy the attributes are used to encrypt the data and a secret key consisting of user attributes to decrypt the data and is used as an access policy in order to restrict the access of the user. This requires flexible and accessible cryptographic key management to support difficult access policies. The scheme is efficient and flexible because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one Cipher text such that only the users whose attributes satisfy the access policy can decrypt the Cipher text.

Keywords: TPA, Trust Party Auditor, Cloud computing, CP-ABE, Access Control

I. INTRODUCTION

Content sharing environments such as social networking are very dynamic in terms of the number of on-line users, storage requirement, network bandwidth, computational capability, applications and platforms, thus it is not easy for a service provider to allocate resources following the traditional client-server model. Cloud computing offers the abstract view to the users and developers as it hides many of the implementation details. It is mainly used in content sharing networks. Examples of these networks are social networking where they are dynamic in terms of storage required. However, due to the weak security issues the use of cloud is not very fast in content sharing networks. Access policy is a mechanism that provides security facilitates the data to user in acontrolled manner. In many situations, when a user encrypts sensitive data, it is imperative that she establish a specific access control policy on who can decrypt this data. For example, suppose that the FBI public corruption offices in Knoxville and San Francisco are investigating an allegation of bribery involving a San Francisco lobbyist and a Tennessee congressman. The head FBI agent may want to encrypt a sensitive memo so that only personnel that have certain credentials or attributes can access it

The data owners encrypt the data using this user public key and then upload the file to the cloud. The user whenever wanted to download the file should decrypt the file with his generated secret key (Using ABE). Hence for a particular shared data among the multiple users we need toencrypt the data with every user's public key in order to provide security hence an ordinary encryption isunsatisfactory. Instead if the cipher text consists of the set of attributes then by using the key and access policy we candecrypt the data i.e. the key works only when the attributes in the cipher text satisfies the access policy.However in orderto design an access policy mechanism there are manychallenges to overcome some of them are (1)user canupload any kind of data like text, media etc.(2) any cangive any number of attributes and hence two or more usersmay have same attributes. (3) Any individual may grand anykind of access to any number of users.This approach allows the user to implement the accesscontrol on their data directly in content sharing servicerather than through a central administrator. Inorder toprovide a complex access policy mechanism we needflexible and scalable cryptographic key managementtalgorithms. To overcome these disadvantages we areusing attribute based encryption .hence we employee CPABE (cipher text policy – attribute based encryption) technique as a remedy to the above mentioned problem inCP-ABE the recipient can decrypt the data only when theuser attribute satisfy the access policy and this can be seenas one-to-many public key encryption and the data ownerprovides access to many users. CP-ABE scheme is similar to the KP-ABE(key policy attribute-based encryption).in keypolicy attribute based scheme the access policy is built-in the users secret key where as in CP-ABE (ciphertext policy attribute based encryption) the access policy is switched into the encrypted data and theattributes are linked with the public key of the user inorder to decrypt the data. If the attribute set in the users secret key satisfies the access policy present in theencrypted data then the data will be decrypted.

II. RELATED WORK

The traditional access control architectures usually assume the data owner and the servers storing the data are in the same trusted domain, where the servers are fully entrusted as an omniscient reference monitor responsible for defining and enforcing access control policies. This assumption, however, no

©IJRASET (UGC Approved Journal): All Rights are Reserved

Longer holds in cloud computing since the data owner. Furthermore, we observe that there are also cases in which cloud users themselves are content providers.

They publish data on cloud servers for sharing and need fine grained data access control in terms of which user (data consumer) has the access privilege to which types of data. In contend-based access control, individuals are explicitly authorized to access collections of records matching certain criteria. We refer to these as collections as content slices. This approach supports individuals who do not have precisely defined roles, such as contractors or medical researchers.

Cloud-based multimedia content sharing is one of the most significant services in cloud-based multimedia systems. In some security and privacy issues of multimedia services are proposed by exploring the multimedia-oriented mobile social network. The relationship between the user identification and resource in content sharing applications is dynamic. There are twoformsof access management strategies they're user attribute access management structure and Media Structure minded Access management structure

Fundamental to usage control model is the concept of attributes attached to both users and resources. In content sharing applications, as mapping between user identity and resource is dynamic, access control methods related to our work can be classified into two categories.

A. User attribute access management structure

Easier [9] is a design that supports fine-grained access control policies and dynamic cluster membership by victimization CP-ABE theme. A lot of works are projected to style versatile ABE schemes There are two methods to comprehend the fine-grained access management supported ABE they are KP-ABE and ABE. In KP-ABE the cipher text consist of some descriptive attributes which are labeled by the sender and the trusted authority issues a user's private key and the access policy is involved in the private key which specifies the decryption of the cipher text with the key. Here the disadvantage of this encryption is that the access policy is constructed into user's personal key. So data owner does not have the option on who can decrypt the data except encrypting the data with the set of attributes. Hence it is not suitable for certain applications as the information owner must trust the authority who gives the user's key. The KP-ABEis secure beneath the final cluster model because it is monotonic access structure and additionally it cannot categorical the attributes to reject the parties with whom the knowledge owner didn't have to share the knowledge from membership. To overcome this weakness cipher text policy attribute based encryption has been created that is proved to be secured below the quality model. In CP-ABE the access policy is made within the encrypted data and also the attributes is with the user's private key. The attribute based encryption will be divided into monotonic or nonmonotonicbased on the sort of the access structure and based on the access policy the schemes will be classified as key policy or cipher text policy. The ideal attribute based encryption must support data privacy, scalability, fine-grained access control, user accountability, user revocation and collusion resistant. But the provided access policies are not appropriate for the scalable media content.

B. Media structured access control

For a video the secure scalable streaming is the progressive encryption technique. This should be integrated with error correction technique since it may result in decryption failure due to the packet loss. An access control scheme is designed by wuetal which is highly secured and efficient and predominantly the scheme is flexible as its "encrypt once, decrypt many ways" is compatible with the features of jpeg 2000.

ABE is adopted to share scalable media based on the attributes rather than the names of the consumers. Some works focus on dealing with the security issues in wireless sensor networks [23], [24] and crowd sourcing networks which is important in multimedia data collection and transmission.

C. Modules

1) Registration
2) Attribute oriented access control
3) One-way hash function
4) Cipher-text policy attribute-based encryption

Modules Description Registration In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader has access to [5].

©IJRASET (UGC Approved Journal): All Rights are Reserved

PUD - public domains

PSD - personal domains

AA - attribute authority

MA-ABE - multi-authority ABE

KP-ABE - Key Policy Attribute based Encryption

MCP-ABE - Multi-message Cipher-text Policy Attribute-Based Encryption

Attribute oriented access control in this Module, supports fine-grained access control policies and dynamic group membership6 by using CP-ABE scheme. In addition, is able to revoke a user without issuing new keys to other users or re-encrypting existing cipher-texts by using a proxy. KP-ABE (Key Policy Attribute based Encryption) to enforce access policies based on data attributes. One-way hash functionin this Module, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.

Cipher-text policy attribute-based encryption in this Module, every user's personal secret key is associated with a set of attributes while every ciphertext is associated with an access policy. A user successfully decrypts a ciphertext only if her set of attributes satisfies the access policy specified in the ciphertext. We briefly describe the CP-ABE. We will extend this CP-ABE scheme to MCP-ABE scheme and use the latter in our access control scheme.

D. Advantages & Limitations:

1) Advantages

a) The scheme has several benefits that ensure password complexity and security control over the sharable data.

b) The present scheme is also secured against user collusion attacks due to use of attribute-based encryption.

c) We present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery.

2) Limitations

a) In an existing system solution is flexible, but it is vulnerable to collusion attack.

b) The existing method is to classify users into different roles based on their attributes, assign role keys to users and then encrypt the content using the role keys. However this approach results in high complexity

III. METHODOLOGY

Cloud computing is an emerging computing paradigm that brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well. In content sharing applications like social networking media, the mapping between user identity and resource is dynamic, access control methods related to our work can increase the security level against user collusion attacks due to use of attribute-based encryption. So the fundamental policy is to implement a control model where we can provide attributes attached to both users and resources. In online content sharing applications, as a mapping between user identity and resource is dynamic, access control methods related to our work can be implemented using the following steps for more secured content sharing. Components in an attribute -based access control scheme includes subjects each specified by a set of attributes, objects and access policies. Attribute Authority (AA), a trusted third party, sets up the system parameters of attribute-based encryption system (such as system-wide public key and master key), and verifies every user's attribute (e.g., group membership, role, and security clearance or authorization information) and issues personal secret key corresponding to the set of attributes of the user. In practice, there could be multiple AAs in a system. For example, a university or corporate may run an AA, and a user may act as an AA for his/her extended family members

IV. PROPOSED WORK

Here we are providing better security in owner's upload side as well as on the download side. For better security client splitting that single file into nine different blocks and providing a unique identification number for each block.

©IJRASET (UGC Approved Journal): All Rights are Reserved

A. One-way hash function

In this Module, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message. Let us assume that is the input and by applying hash function the output will be Y i.e. H(X) =Y. It is impossible to obtain the reimage X from the image Y. An example for one way hash function is SHA-1 and MD-5.

B. Cipher-text policy attribute-based encryption

In this Module, every user's personal secret key is associated with a set of attributes while every ciphertext is associated with an access policy. A user successfully decrypts a cipher text only if her set of attributes satisfies the access policy specified in the ciphertext. We briefly describe the CP-ABE. We will extend this CP-ABE scheme to MCPABE scheme and use the latter in our access control scheme.

1) *AB-Setup:* It is an initialization algorithm run by an Attribute Authority (AA). It takes as input a security and outputs a public key PK and a master secret key.
2) *AB-Encrypt:* nData owner to encrypt a message according to an access tree.
3) *AB-Decrypt:* Data consumer in possession of a set of attributes a and the secret key SK in order to decrypt the cipher-text CT with an access policy.

V. CONCLUSION

CP-ABE primarily based access management permits data owner to enforce access management supported attributes of data customers while not explicitly naming the particular information customers. However, CP-ABE supports just one privilege level and therefore isn't suitable for access management to ascendable media. Cloud computing is the highly adaptive technology and mobile devices are becoming widespread the above presented CPABEaccess control helps to free from the computational demanding operations on the cloud server. With the assistance of the cloud the acceleration of the decryption increased but it is still slow in some lowed devices because anintegrated exponentiation operation is required.CP-ABE supports only one privilege level and hence is not suitable for access control to scalable media. In this paper we extended CP-ABE to a novel MCP-ABE and proposed a scheme to support multi-privilege access control to scalable media.

In this paper we extended CP-ABE to a novel MCP-ABE and proposed a scheme to support multi-privilege access control to scalable media. As cloud computing is increasingly being adopted and mobile devices are becoming pervasive, the present access control scheme allows a mobile user to offload computational intensive MCP - ABE operations to cloud servers while without compromising user's security.

Below are the main points that can be concluded after the experimental sharing of image, audio and video to the group of limited users.

A. The scheme has several benefits that ensure password complexity and security control over the sharable data.
B. The present scheme is also secured against user collusion attacks due to use of attribute-based encryption.
C. We present an access control scheme for scalable media. The scheme has several benefits which make it especially suitable for content delivery.

VI. FUTURE SCOPES

We propose a privacy-preserving public auditing mechanism for shared data in the cloud allows a verifier to check the correctness of a client's data stored at an untrusted server. By utilizing RSA-based homomorphism authenticators and sampling strategies, the verifier is able to publicly audit the integrity of data without retrieving the entire data, which is referred to as public auditing. Unfortunately, their mechanisms only suitable for auditing the integrity of personal data. Similar model called Proofs of Irretrievability (POR), which is also able to check the correctness of data on an untrusted server. The original file is added with a set of randomlyvaluedcheck blocks called sentinels. The verifier challenges the untrusted server by specifying the positions of a collection of sentinels and asking the untrusted server to return the associated sentinel values. Sachem and Waters designed two improved schemes. The first scheme is built from BLSsignatures, and the second one is based on pseudo-random functions. We utilize ring signatures to constructhomomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each.

©IJRASET (UGC Approved Journal): All Rights are Reserved

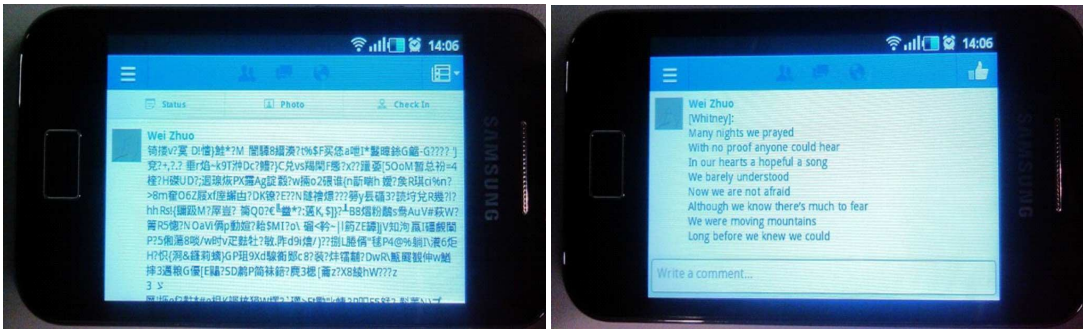
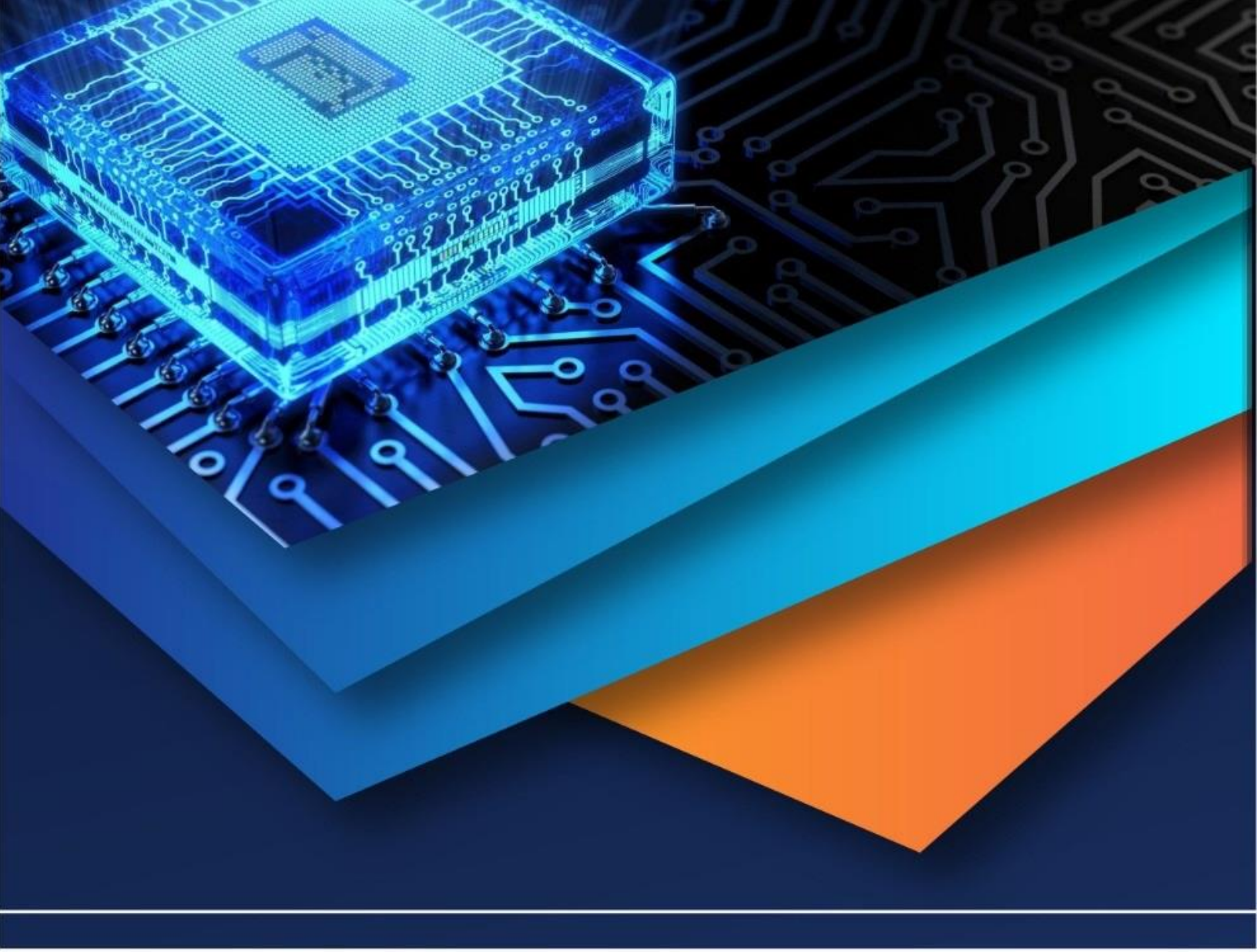


Fig .A) After Encryption B) Before Encryption

REFERENCES

[1] Yongdong Wu, Zhou Wei, and Robert H. Deng "Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks"- IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 15, NO. 4, JUNE 2013.
[2] Priya A. Kamble,PragatiPatil " Attribute-Based Access To Multimedia In Cloud-Assisted Online Content Sharing "-IEEE Volume 5, Issue 10, October-201
[3] V Benzoic, D Sock, R Steinhardt, and V. I. Val- lanai, \Multiauthority Attribute-based encryption with honest-but-curious central Authority," International Journal of Computer Mathematics, vol. 89, pp. 3, 201
[4] Journal & Magazine of Engineering, Technology, Management and Research A PeerReviewed Open Access International JournalISSN No: 2348-4845 Volume No: 2 (2015), Issue No: 6 (June) June 201
[5] Scalable Media in Cloud-assisted Content Sharing with Attribute-based Access Networks Maheswararao.N1, Sk.N.Rehmathunnisa2, IJCSIET-ISSUE5-VOLUME3-SERIES1
[6] CIPHER-Text Policy Attribute Based Access to Cloud,Venkateshprasad.Kalluri et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2796-2799,
[7] Ciphertext-Policy Attribute-Based Encryption Authorized licensed use limited to: Unit of Calif Los Angeles. Downloaded on July 27, 2009 at 19:33 from IEEE Explore
[8] Hash-based Digital Signature Schemes, October 29, 2008.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)